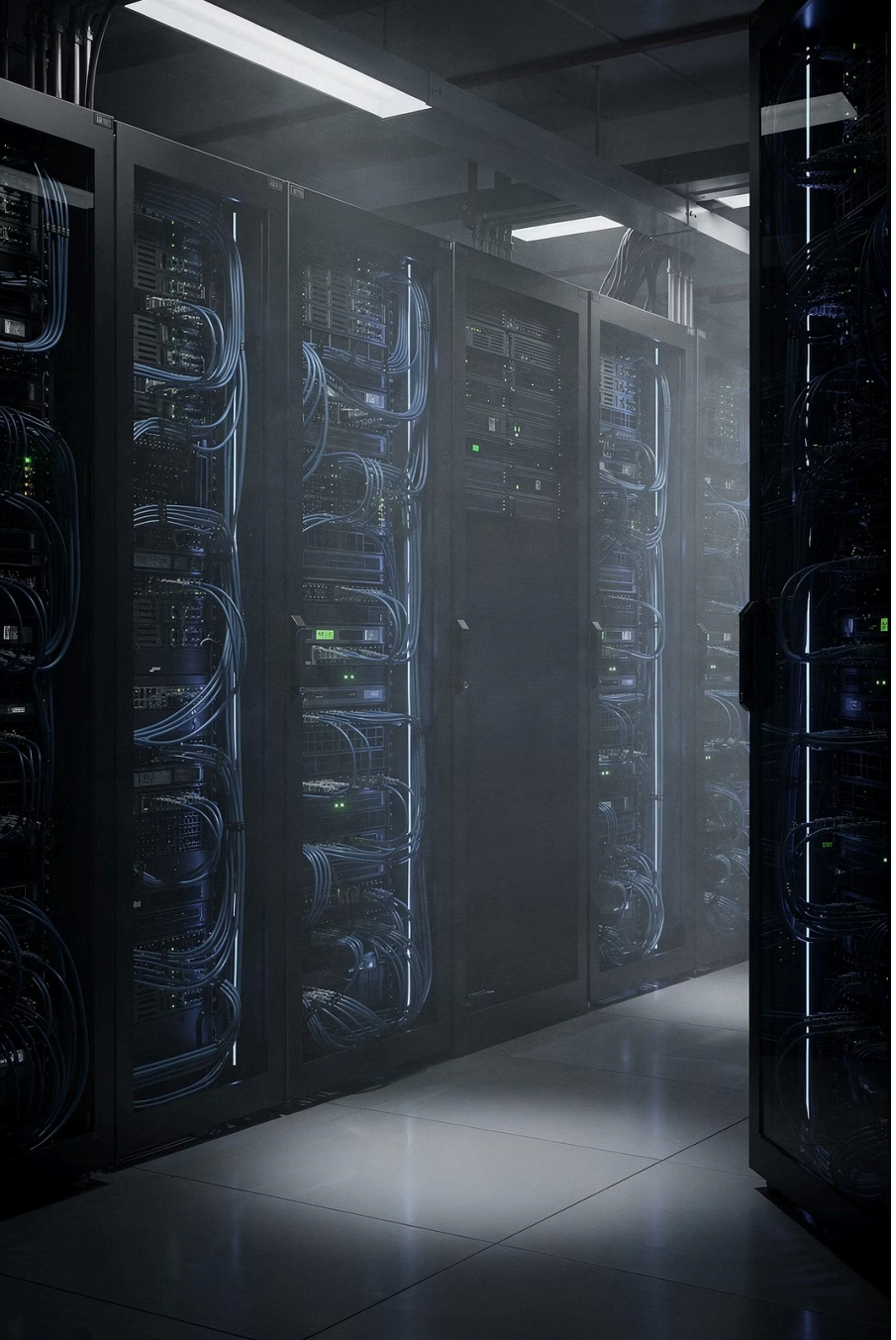


Modul 2: Reconnaissance & Information Gathering

Temukan "permukaan serangan" secara sistematis — fondasi utama setiap aktivitas bug bounty yang sukses.

C-SIX SECURITY

EDY SUSANTO — FOUNDER

Tujuan Pembelajaran

Apa yang Akan Kamu Capai?

Di akhir modul ini, peserta mampu mengidentifikasi dan memetakan permukaan serangan sebuah organisasi secara metodis. Reconnaissance yang baik adalah penentu kualitas temuan bug bounty — semakin dalam recon, semakin besar peluang menemukan celah yang luput dari perhatian orang lain.

🔍 Temukan

Subdomain, aset, dan infrastruktur tersembunyi milik target

🗺️ Petakan

Seluruh aset organisasi dalam satu gambaran attack surface

🎯 Identifikasi

Teknologi, stack, dan titik lemah potensial secara sistematis

Mindset Recon Hunter

Seorang recon hunter tidak hanya mencari — ia **berpikir seperti penyerang**. Setiap domain, IP, atau nama karyawan adalah petunjuk yang bisa membuka jalur baru. Pendekatan yang sabar, metodis, dan kreatif adalah kunci membedakan hunter biasa dari hunter yang selalu menghasilkan temuan.

Kuriositas Tinggi

Selalu bertanya "apa lagi yang tersembunyi?" di balik setiap data yang ditemukan.

Dokumentasi Terstruktur

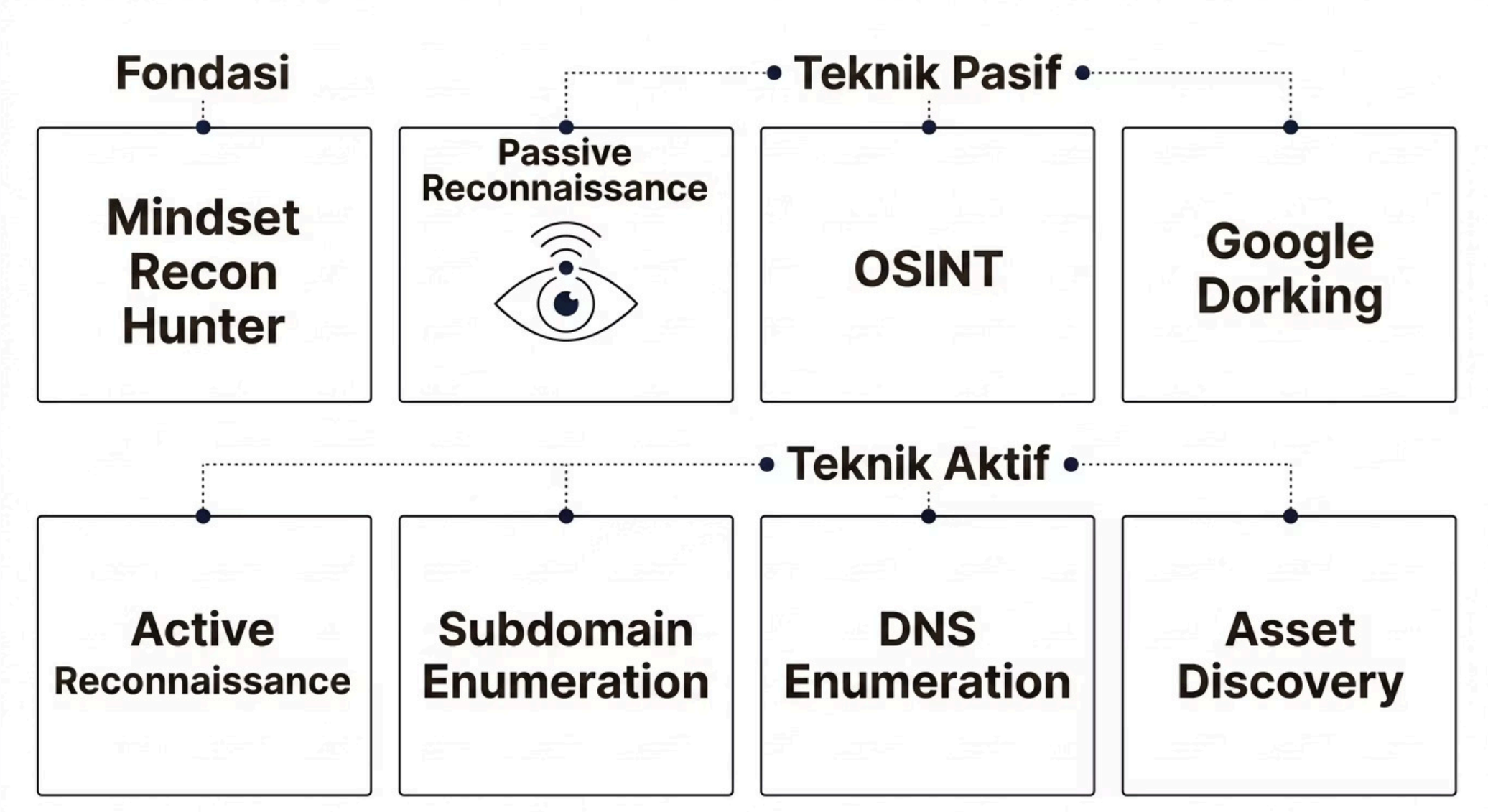
Catat setiap temuan sekecil apapun. Data yang tampak tidak relevan hari ini bisa krusial esok.

Berpikir Lateral

Hubungkan titik-titik informasi untuk menemukan pola dan celah yang tidak terlihat langsung.

Peta Materi Modul 2

Modul ini mencakup delapan topik utama yang saling berkaitan, mulai dari fondasi mindset hingga teknik lanjutan seperti OSINT dan Google Dorking.



Passive Reconnaissance

Mengintai Tanpa Terdeteksi

Teknik passive recon dilakukan **tanpa berinteraksi langsung** dengan sistem target. Tidak ada paket yang dikirim ke server mereka — identitas hunter tetap tersembunyi sepenuhnya.

Apa saja yang bisa dikumpulkan?

- Informasi WHOIS dan data registrasi domain
- Rekaman DNS historis dan zona transfer
- Data dari mesin pencari dan cache publik
- Profil perusahaan dari LinkedIn, GitHub, dan media sosial
- Dokumen publik yang mengandung metadata sensitif
- Informasi leak dari breach database publik

Active Reconnaissance

Berbeda dengan passive recon, teknik **active reconnaissance** melibatkan interaksi langsung dengan sistem target. Ini berarti jejak aktivitas dapat tercatat di log server — lakukan hanya pada target yang sudah masuk dalam scope program bug bounty.

01

Port Scanning

Identifikasi port terbuka dan layanan yang berjalan menggunakan Nmap atau Masscan.

02

Service Fingerprinting

Tentukan versi software dan teknologi yang digunakan untuk menemukan CVE relevan.

03

Web Crawling

Jelajahi struktur aplikasi web untuk menemukan endpoint, parameter, dan direktori tersembunyi.

04

Directory Brute-forcing

Gunakan wordlist untuk mengungkap halaman admin, backup file, dan panel tersembunyi.

Subdomain Enumeration

Subdomain adalah salah satu sumber **temuan bug bounty terkaya**. Banyak subdomain staging, dev, atau legacy yang terlupakan oleh tim keamanan dan mengandung kerentanan serius. Tujuannya adalah menemukan seluruh subdomain yang terkait dengan domain utama target.

Kombinasi teknik pasif dan aktif menghasilkan cakupan subdomain yang jauh lebih komprehensif dibanding menggunakan satu metode saja.

DNS Enumeration

Membaca Peta Infrastruktur

DNS adalah "buku telepon" internet — memetakan nama domain ke alamat IP. Enumerasi DNS yang teliti dapat mengungkap struktur internal jaringan, layanan email, CDN yang digunakan, hingga IP address yang menjadi target sesungguhnya di balik layanan proteksi seperti Cloudflare.

- **A / AAAA Record** — IP address server
- **MX Record** — server email organisasi
- **TXT Record** — verifikasi layanan, SPF, DKIM
- **CNAME Record** — subdomain takeover opportunities
- **NS Record** — nameserver dan registrar

ℹ 💡 **Subdomain Takeover**

CNAME yang mengarah ke layanan pihak ketiga yang sudah tidak aktif (seperti Heroku, GitHub Pages) dapat diambil alih oleh penyerang — ini adalah temuan high-severity yang sering ditemukan lewat DNS enumeration.

⚠ ⚠️ **Zone Transfer**

Beberapa DNS server yang salah konfigurasi mengizinkan AXFR request, membocorkan seluruh record DNS internal organisasi sekaligus.

Asset Discovery

Asset discovery melampaui subdomain — tujuannya adalah memetakan **seluruh jejak digital** sebuah organisasi: IP ranges, ASN, cloud buckets, API endpoints, aplikasi mobile, dan repositori kode publik. Semakin lengkap peta aset, semakin besar peluang menemukan titik lemah yang diabaikan.

Cloud Assets

S3 buckets, Azure Blobs, dan GCP storage yang salah konfigurasi sering mengekspos data sensitif secara publik.

Source Code

Repositori GitHub/GitLab publik milik perusahaan bisa mengandung API key, credential, dan endpoint internal.

Mobile Apps

APK dan IPA dari aplikasi publik dapat di-decompile untuk menemukan endpoint API tersembunyi.

Open Source Intelligence

OSINT — Kekuatan Data Publik

OSINT adalah seni mengumpulkan dan menganalisis informasi yang tersedia secara publik untuk membangun gambaran lengkap tentang target. Dalam konteks bug bounty, OSINT membantu menemukan aset yang tidak terdaftar resmi, mengidentifikasi teknologi stack, bahkan menemukan credential yang bocor.

Shodan & Censys

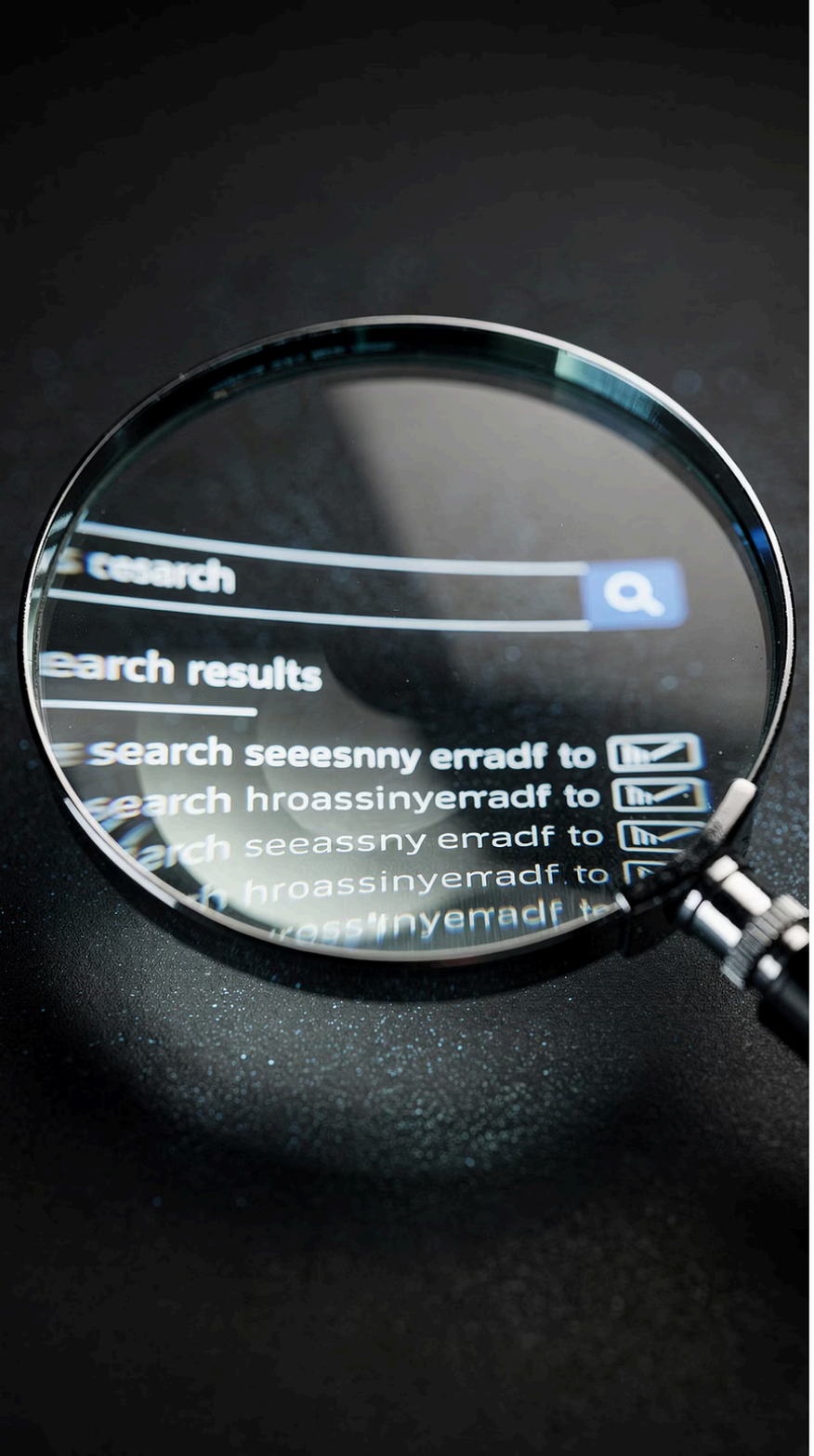
Mesin pencari khusus untuk perangkat yang terhubung ke internet. Temukan server, IoT, dan layanan yang terekspos beserta banner informasinya.

LinkedIn & Social Media

Profil karyawan mengungkap teknologi yang digunakan perusahaan, nama sistem internal, dan target potensial untuk social engineering.

Breach Databases

Layanan seperti HaveIBeenPwned dan DeHashed membantu menemukan email dan password yang pernah bocor dari domain target.



Google Dorking

Google Dorking memanfaatkan **operator pencarian lanjutan Google** untuk menemukan informasi sensitif yang secara tidak sengaja terindeks oleh mesin pencari. Teknik ini adalah salah satu yang paling powerful dalam passive recon dan sering menghasilkan temuan langsung tanpa perlu menyentuh target.

site:

Batasi pencarian ke domain tertentu.
site:target.com filetype:pdf

inurl:

Cari kata kunci di URL.
inurl:admin site:target.com

intitle:

Cari kata kunci di judul halaman.
intitle:"index of" site:target.com

filetype:

Temukan jenis file tertentu.
filetype:env site:target.com

Arsenal Tools

Tools Wajib Recon Hunter

Berikut adalah toolkit inti yang digunakan oleh professional bug bounty hunter di seluruh dunia. Kuasai setiap tool ini dan pahami kapan harus menggunakannya.

Subfinder

Fast passive subdomain discovery dari berbagai sumber publik. Output bersih, mudah di-pipe ke tool lain.

Amass

Tool OWASP yang komprehensif untuk network mapping dan external asset discovery. Kombinasi pasif dan aktif.

Assetfinder

Tool ringan buatan tomnomnom untuk menemukan domain dan subdomain terkait dengan target dengan cepat.

Whois

Mengungkap data registrasi domain: pemilik, registrar, nameserver, dan tanggal kedaluwarsa.

Shodan

Mesin pencari untuk perangkat internet. Temukan server, kamera, dan layanan terekspos milik target.

Sesi Praktik

Pengetahuan tanpa praktik hanyalah teori. Pada sesi praktik ini, peserta akan menjalankan langsung ketiga tugas berikut menggunakan tools yang telah dipelajari. Dokumentasikan setiap langkah dan temuan dalam catatan recon kalian.

Praktik 1 — Subdomain Hunting

Gunakan Subfinder, Amass, dan Assetfinder untuk menemukan subdomain dari target yang ditentukan. Bandingkan hasil ketiga tools dan gabungkan outputnya.

Praktik 2 — Asset Mapping

Petakan seluruh aset digital organisasi target: IP range, ASN, layanan cloud, dan repositori publik menggunakan kombinasi Shodan dan WHOIS.

Praktik 3 — Tech Identification

Identifikasi teknologi yang digunakan website target: framework, CMS, CDN, server, dan library JavaScript menggunakan Wappalyzer dan header analysis.

Workflow Profesional

Recon Pipeline yang Efektif

Hunter berpengalaman tidak bekerja secara ad-hoc — mereka memiliki **pipeline yang terstruktur dan dapat diulang** untuk setiap target baru. Otomasi dan dokumentasi adalah kunci efisiensi.

Pro Tip: Simpan semua output ke file dan gunakan tools seperti anew untuk menghilangkan duplikat secara otomatis saat menggabungkan hasil dari berbagai tools.

Contoh One-Liner Pipeline

```
subfinder -d target.com -silent \
  | anew subdomains.txt

amass enum -passive \
  -d target.com \
  | anew subdomains.txt

cat subdomains.txt \
  | httpx -silent \
  | anew live_hosts.txt
```

Pipeline ini secara otomatis mengumpulkan subdomain dari beberapa sumber dan menyaring hanya host yang aktif dan merespons HTTP.

Outcome & Kesimpulan Modul 2

Setelah menyelesaikan Modul 2, peserta telah memiliki kemampuan dasar seorang recon hunter profesional. Ingat — **recon yang baik adalah 70% dari keberhasilan bug bounty**. Investasikan waktu lebih banyak di sini sebelum melangkah ke tahap eksploitasi.

✅ Mampu Melakukan

- Subdomain enumeration sistematis
- DNS analysis & zone transfer check
- OSINT & Google Dorking
- Asset mapping organisasi

🛠️ Tools Dikuasai

- Subfinder, Amass, Assetfinder
- Whois & DNS tools
- Shodan
- Google Dork operators

➡️ Modul Berikutnya

Modul 3 akan membahas **Vulnerability Assessment** — cara menganalisis temuan recon untuk mengidentifikasi kerentanan yang dapat dieksploitasi dan dilaporkan.

Edy Susanto — Founder C-SIX Security